Jeffrey L. Poston
JPoston@crowell.com
(202) 624-2775 direct

Crowell & Moring LLP
1001 Pennsylvania Avenue NW
Washington, DC 20004
+1.202.624.2500 main
+1.202.628.5116 fax

August 9, 2024

Hon. Ramon E. Reyes, Jr.
District Court Judge
U.S. District Court
Eastern District of NY

RE: *Microsoft Corp. et al.* v. *John Does 1-16*, Case No. 23-cv-2447-RER-LKE

Dear Judge Reyes, Jr.:

Plaintiffs Microsoft Corporation ("Microsoft"), Fortra LLC ("Fortra"), and Health-ISAC, Inc. ("Health-ISAC")[1] (collectively "Plaintiffs"), by and through their counsel, submit this letter motion to respectfully request reconsideration of the Clerk's denial of Plaintiffs' Request for Certificate of Default, which was denied on grounds that the John Doe Defendants have not been identified by first and last name.

The granting of the Request for Certificate of Default is proper in this matter because (i) Defendants are aware of these proceedings, have received full due process and have chosen not to respond to this action for fear of being arrested and/or prosecuted, (ii) Defendants are prolific cybercriminals who purposefully mask their identities online and consequently, are rarely identified by their full name, and (iii) there is long standing precedent for granting default judgment against unnamed defendants in similar cybercrime circumstances.

I. Factual Background

The John Doe Defendants are prolific cybercriminals who purposefully obfuscate their identities as they launch cyberattacks against domestic and foreign victims with a special focus on the health care industry. This action arose as a result of Defendants' theft and misuse of a penetration testing tool manufactured by Plaintiff Fortra LLC known as Cobalt Strike. Cobalt Strike is a software program that permits companies to assess their cyber defenses through a means known as "penetration testing," which simulates cyberattacks permitting the user to identify and remediate cyber vulnerabilities.

[1] Health-ISAC is a membership organization comprised of various health care providers, hospitals, health insurance companies, pharmaceutical companies, medical schools, and medical R&D organizations. Health-ISAC represents the interests of its healthcare industry members in combating and defending against cyber threats that pose risk and loss to the healthcare industry.

The John Doe Defendants stole or otherwise illegally procured the Cobalt Strike software and then used the stolen copies of software for illegal purposes, including perpetrating devastating malware and ransomware attacks, and infringing Microsoft's and Fortra's proprietary software.

The John Doe Defendants illegally created an unauthorized ("cracked") version of the Cobalt Strike tool[2] to lure unsuspecting users into obtaining and downloading this cracked version. When a user implements the cracked version on its systems, the John Doe Defendants are able to take control of the victims' computers and steal sensitive information, launch malware and ransomware attacks, and hold the victims' computers hostage. Through the cybercriminal organization that John Doe Defendants are a part of, they are able to leverage some of the most prolific and dangerous ransomware, including Conti, LockBit, Quantum Locker, Royal, Cuba, BlackBasta BlackCat and PlayCrypt. Dkt. 1 (Complaint), ¶ 37.

In connection with these attacks, Defendants violate Microsoft's intellectual property rights. For example, the Defendants infringe Microsoft's copyrighted computer code when they take control of victims' computers that use a Microsoft operating system. Complaint, ¶ 76. This infringement allows Defendants to change Microsoft user settings and take control of the operating system. *Id.* In many instances, the victim is unaware that John Doe Defendants have taken over their computers until it is too late—e.g., John Doe Defendants delete the users' files and then demand ransom to recover the files. *Id.* ¶ 137. In those instances, not only has Microsoft's IP been infringed, but the victims mistakenly believe that Microsoft is responsible for the attack. *Id.* ¶ 77. In other instances, because the compromised Windows operating system does not appear to be different that the uncompromised version, a user may think that the compromised operating system was actually developed by Microsoft. *Id.* This causes irreparable harm to Microsoft's reputation and goodwill, which Microsoft has spent considerable resources developing. *Id.* ¶ 95.

These Defendants and their affiliated criminal organizations leverage cracked Cobalt Strike to attack hospitals and other healthcare facilities throughout the United States and in this judicial district.[3] Dkt. 2-6 (Declaration of Health-ISAC) ¶¶ 14-15. These attacks on hospitals, including those located in this district have caused the following consequences: disrupting patient care, shutting down access to electronic health records, delays in diagnostic, imaging, and laboratory results, and exposing patient data of millions of patients. *Id.* And worldwide, John Doe Defendants have employed the same strategy: leveraging Cobalt Strike as the delivery mechanism for prolific ransomware attacks.[4]

[2] Because the Cobalt Strike software offered by Fortra is a legitimate cyber security tool, Plaintiffs have used the term "cracked Cobalt Strike" to refer to stolen, unlicensed, or otherwise unauthorized copies of the software that John Doe Defendants have stolen.

[3] John Doe Defendants do not confine their attacks to hospitals, they have used cracked Cobalt Strike to deliver ransomware and malware to numerous computers in this district. Complaint, ¶ 26.

[4] For example, as Plaintiffs alleged in the Complaint, in 2021, cybercriminals attacked the Ireland Health Service Executive using the Conti ransomware. A post attack investigation revealed that cracked versions of Cobalt Strike were used to carry out the cyberattack. As a result of the attack, key health systems were taken offline, which caused significant patient care disruption. Health-ISAC Declaration, ¶ 11.

Unsurprisingly given John Doe Defendants prolific criminal activity, Defendants intentionally obfuscate their identities in order to continue their criminal activities, and to evade arrest or prosecution. This has made identification of their names and locations for service challenging, particularly where Defendants may be foreign actors. As other courts in this Circuit have recognized, Article 1 of the Hague Convention specifies that the Convention does not apply when the addresses of the foreign defendants are unknown. *See SEC v. Lines*, 2009 U.S. Dist. LEXIS 91811, *9 (S.D.N.Y. Oct. 2, 2009) (Cote, J.) ("[The Hague Convention] 'shall not apply where the address of the person to be served with the document is not known.'")

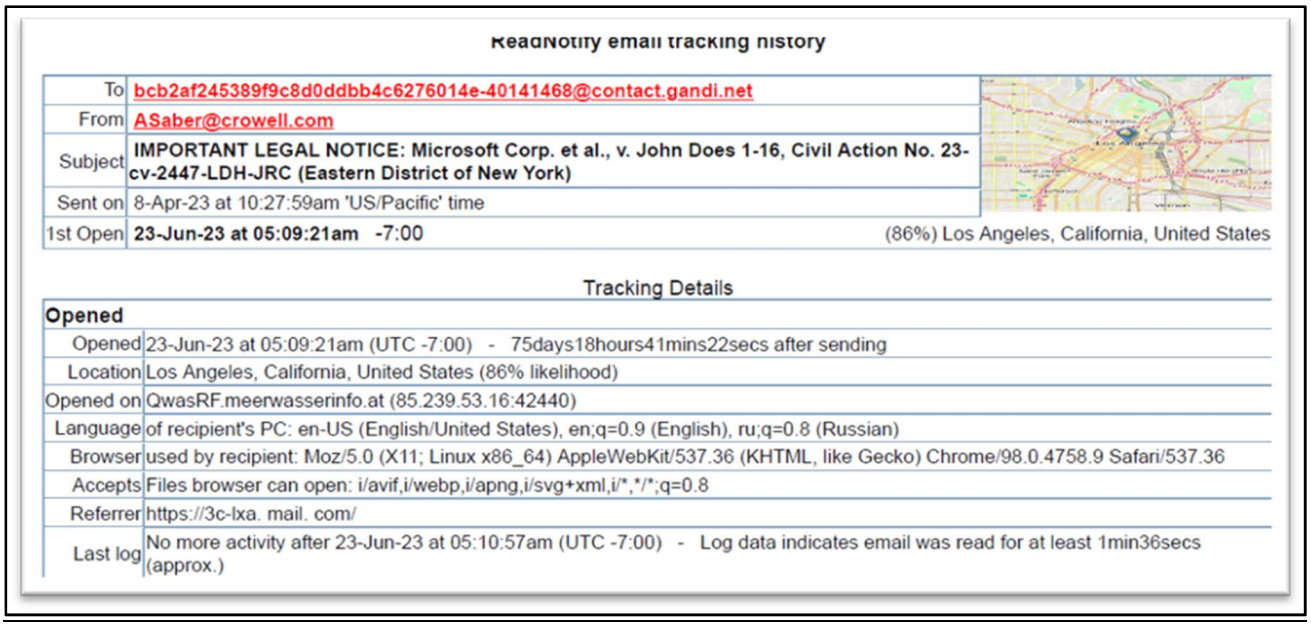
Defendants operate via the Internet and usernames, and use sophisticated means to conceal their identities and locations. Plaintiffs endeavored to identify Defendants and their locations through discovery as granted by the Court and served subpoenas on third parties to ascertain additional information. Microsoft analyzed the information received in response to the subpoenas and determined that John Doe Defendants used aliases and false information in order to anonymize their activities. For example, the emails address that they provided to register a domain were from anonymous email account providers like ProtonMail that obscure the identity of the account holder. Plaintiffs have been unable to specifically and definitively determine the "real" names and physical addresses of Defendants on account of their deliberate efforts to obfuscate their identities.

II. Procedural History

On March 30, 2023, Plaintiffs brought this action, alleging violations of the Digital Millennium Copyright Act, Electronic Communications Privacy Act, the Racketeer Influenced and Corruptions Act, copyright infringement, trademark infringement and common law trespass to chattels, conversion, and unjust enrichment. Plaintiffs also sought a temporary restraining order aimed at shutting down the technical infrastructure (including website domains and IP addresses) that John Doe Defendants use to carry out their criminal attacks in this jurisdiction as well as other parts of the United States. Plaintiffs' TRO was supported by declarations from Microsoft, Fortra, and Health-ISAC, including detailed technical declarations explaining how Plaintiffs were able to identify and attribute the technical infrastructure to John Doe Defendants. See Dkt. 2-1, 2-2, 2-3, 2-4, 2-5, and 2-6. On March 31, 2023, the Court granted Plaintiffs' request for a TRO, ordering the transfer of the domains and the blocking of IP addresses that John Doe Defendants use to carry out their attacks. Dkt. 13. The Court specifically found that Plaintiffs were likely to prevail on each of their claims. *Id.* at p. 4. Additionally, the Court authorized alternative service given that John Doe Defendants' *modus operandi* is to obfuscate their identity and avoid detection. *Id.* at p. 7, 12. Finally, the Court ordered that Defendants file with the Court any response by April 12, 2023 and ordered them to appear on April 13, 2023 to show cause, if any, why the Court should not enter a Preliminary Injunction. *Id* at 13.

Plaintiffs served John Doe Defendants via email service (using the email addresses that Defendants used to register the domains the John Doe Defendants use and leverage as part of their attacks) and publication on April 3, 2023. Plaintiffs' counsel used a service known as ReadNotify to track whether the service emails were delivered. By appending ".readnotify.com"

to the end of each of the registrant emails, counsel is able to track the correspondence, including when the email is received and when it is viewed (to the extent that it is viewed). Plaintiffs' counsel confirmed using ReadNotify that the service emails were delivered and, in some instances, opened. Figure 1 is an example of someone affiliated with an email address that John Doe Defendants used to register a domain opening the service email sent by Plaintiffs' counsel.



ReadNotify email tracking history

To	bcb2af245389f9c8d0ddbb4c6276014e-40141468@contact.gandi.net
From	ASaber@crowell.com
Subject	IMPORTANT LEGAL NOTICE: Microsoft Corp. et al., v. John Does 1-16, Civil Action No. 23-cv-2447-LDH-JRC (Eastern District of New York)
Sent on	8-Apr-23 at 10:27:59am 'US/Pacific' time
1st Open	**23-Jun-23 at 05:09:21am** -7:00 (86%) Los Angeles, California, United States

Tracking Details

Opened	
Opened	23-Jun-23 at 05:09:21am (UTC -7:00) - 75days18hours41mins22secs after sending
Location	Los Angeles, California, United States (86% likelihood)
Opened on	QwasRF.meerwasserinfo.at (85.239.53.16:42440)
Language	of recipient's PC: en-US (English/United States), en;q=0.9 (English), ru;q=0.8 (Russian)
Browser	used by recipient: Moz/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.9 Safari/537.36
Accepts	Files browser can open: i/avif,i/webp,i/apng,i/svg+xml,i/*,*/*;q=0.8
Referrer	https://3c-lxa. mail. com/
Last log	No more activity after 23-Jun-23 at 05:10:57am (UTC -7:00) - Log data indicates email was read for at least 1min36secs (approx.)

FIGURE 1

On April 13, 2023, the Court held a hearing concerning Plaintiffs' request for a preliminary injunction. Defendants failed to appear or file an opposition. The Court granted the preliminary injunction on April 19, 2023, and ordered third party registrars to transfer the website domains that John Doe Defendants use, own, or operate as part of their infrastructure to Microsoft in order to shut down Defendants' ability to carry out future attacks. Dkt. 20.

Subsequently, because John Doe Defendants attempted to rebuild their technical infrastructure, Plaintiffs filed supplemental requests for preliminary injunctions requesting that the Court order the transfer of the additional website domains to Microsoft. Based on the allegation of the Complaint and the supporting declarations from Plaintiffs, the Court granted these motions on June 16, 2023, October 11, 2023, and March 27, 2024. In each instance, Plaintiffs served John Doe Defendants via email service and by publication as authorized by the Court. In each instance, Defendants failed to respond or appear. In the interim, Plaintiffs sought additional discovery from service providers (*e.g.*, the domain registrars), seeking information that would allow Plaintiffs to identify John Doe Defendants. The information that Plaintiffs received did not reveal the identity of the John Doe Defendants.

On July 25, 2024, Plaintiffs requested a certificate of default. Dkt. 44. On August 1, The Clerk of the Court denied the request on grounds that John Doe Defendants were not identified by first and last names. Plaintiffs' counsel understands, based on conversations with the Court

Clerk, that this request was denied without considering the record, the evidence the Plaintiffs have already submitted in support of its claims, and the prior orders of the Court granting Microsoft relief against John Doe Defendants. The Clerk advised Plaintiffs' counsel to file a letter petition directly with the Court.

III. Argument

The Court may make an entry of default against Defendants who fail to plead or otherwise defend actions commenced against them by Plaintiffs, if the Court determines that Defendants have been properly served by Plaintiffs. *See* Fed. R. Civ. P. 55(a).

A. Defendants Have Been Served, Received Actual Notice, and Failed to Respond to the Action

Plaintiffs served Defendants with the Complaint, pleadings, and all key orders in this action pursuant to the means authorized by the Court in the TRO and Order for Preliminary Injunction. This includes service via email through email addresses linked to the domain name registration of the malicious domains and associated IP addresses that are part of the command-and-control infrastructure that proliferates cracked versions of Cobalt Strike.[5]

Plaintiffs also served process by "publishing notice to the Defendants on a publicly available Internet website" as permitted by the TRO and Preliminary Injunction. Dkt. 13 at p.7; Dkt. 20 at p. 7. Furthermore, Plaintiffs know that Defendants received actual notice. In response to Plaintiffs' email serving the Complaint and pleadings to John Doe Defendants, Plaintiffs' counsel received a response from the username "Furry Curry" using the email address "curriculum[@]mail.com with the message "*long live zelenski*." And when Plaintiffs served this new email address, the account holder opened the email, but chose to ignore the notice and service Plaintiffs provided. Indeed, in granting the TRO, the preliminary injunction, and supplemental preliminary injunctions, the Court has acknowledged that Plaintiff's service and notice was proper and adequate. Dkt. 20, ¶ 19.

Despite this robust notice and service and due process, Defendants have not come forward in this action to defend or seek reinstatement of the malicious Cracked Cobalt Strike infrastructure.

B. There is Ample Precedent Granting Default Judgements in John Doe Defendant Cases

This issue is not novel to this Court. Indeed, this Court previously entered default judgments and permanent injunctions on behalf of Microsoft in cases involving John Doe Defendants who were using Microsoft proprietary software to engage in ongoing and damaging cybercriminal activity. For example, in *Microsoft v. John Does 1-2*, Case No. 1:20-cv-01217-LDH-RER (E.D.N.Y) (DeArcy Hall) this court entered default judgment where John Doe Defendants were properly and adequately served and, as here, failed to appear or reveal their identities. Dkt. 22 at p. 3. Indeed, in the Court's report and recommendation, the Court found that because the

[5] Plaintiffs served Defendants by email copies of the complaint, temporary restraining order, preliminary injunction order, supplemental preliminary injunction orders, and a link to a publicly accessible website that published copies of pleadings in this action, on April 3, 2023, May 11, 2023, June 29, 2023, October 30, 2023, and May 21, 2024.

injunction (similar to injunction the Court ordered *in this case*) successfully disrupted John Doe Defendants' technical infrastructure, Defendants are "likely aware" of the impact of these takedown injunctions, and would thus have notice of the action. Dkt. 19 at 5-6. Additionally, the report and recommendation noted that "Microsoft made extensive discovery efforts to obtain the identifies and locations of Defendants to no avail" and found Microsoft's efforts to be sufficient to merit default judgment—even though Microsoft was never able to identity the real names of the Doe Defendants. *Id.* at 8.

Two other cases in this district have ordered the same relief—each in circumstances where Doe Defendants were able to successfully hide their identities: *Microsoft Corporation et al. v. John Does 1-39 et al.*, Case No. 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) and *Microsoft v. John Does 1-5,* 1:15-cv-06565-JBW-LB (E.D.N.Y. 2015).

Beyond *this district*, courts have routinely granted default judgment to Microsoft against John Doe Defendants engaged in cybercriminal acts similar to those at issue in this case: See e.g. *Microsoft Corporation v. John Does 1-27*, Case No. 1:10-cv-00156 (E.D. Va. 2010) (Brinkema, J.); *Microsoft v. John Does, 1-11,* Case No. 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.); *Microsoft Corp. v. John Does 1-18 et al.*, Case No. 1:13-cv-139-LMB/TCB (E.D. Va. 2013) (Brinkema, J.); *Microsoft v. John Does 1-82*, Case No. 3:13-CV-00319-GCM (W.D. N.C. 2013) (Mullen, J.); *Microsoft v. John Does 1-8*, Case No. A-13-CV-1014-SS (Sparks, J.) (W.D. Tex 2013); *Microsoft v. John Does 1-8,* Case No. 1:14-cv-811-LO-IDD (O'Grady, J.) (E.D. Va. 2014); *Microsoft v. John Does 1-3,* Case No. 1:15-cv-240-LMB/IDO (Brinkema, J.) (E.D. Va. 2015); *Microsoft Corporation v. John Does 1-2,* Case No. 1:16-cv-993 (E.D. Va. 2016) (Lee, J.); *Microsoft Corporation v. John Does 1-2*, Case No. 1:19-cv-00716-ABJ (D.C. 2019) (Berman-Jackson, J.); *Microsoft Corporation v. John Does 1-2,* Case No. 1:19-cv-01582 (E.D. Va. 2019) (O'Grady, J.); *Microsoft Corporation and FS-ISAC, Inc. v. John Does 1-2,* Case No. 1:20-cv-1171 (E.D. Va. 2020) (Trenga, J.). In each of these cases Microsoft diligently sought to identify the John Doe Defendants, but the John Doe Defendants were able to successfully avoid identification. In each of these instances, the Court recognized the futility of identifying cybercriminals and granted default judgment relief to Microsoft. Plaintiffs respectfully submit that this Court do the same here and grant the Request for Certificate of Default.

C. Denying the Request for Default Would Unfairly Prejudice the Plaintiffs

Denying the Request for Certificate of Default solely due to the Defendants' unidentified status would unfairly prejudice the Plaintiffs and undermine the judicial process, allowing these bad actors to evade responsibility and liability through their anonymity permitting them to continue their cyber- crimes.

We appreciate the court's consideration of our request and remain available at Your Honor's convenience to confer regarding this matter.

Respectfully submitted,

Jeffrey L. Poston

Counsel for Plaintiffs Microsoft Corp., Fortra LLC, and Health-ISAC, Inc.